3. Admins wary. Flag hunt on!

After previous exploits, trust is scarce. Only trusted admins will receive scan results. Can you still find the flag?

Even with our best efforts, vulnerabilities linger. Your challenge? Probe the tool's defenses, exploit its flaws, and unveil hidden flags.

Challenge

This challenge uses a tool to ping specified hosts, aiming to exploit a command injection vulnerability in the user-supplied domain. Since the application does not provide an output, you need to use the `nslookup` command to send the flag file's content to Burp Collaborator.

- Target Application: Asset Discovery tool
- Initial Endpoint: `http://web0x09.hbtn/app4/`

```
Useful instructions:
1. Log into Asset Discovery tool.
2. ping is vulnerable.
3. We can try and give it an input (google.com for example).
4. Use the nslookup command
5. Flag Location "/var/www/3-flag.txt"
```